JP,05-108487,A(1993) [CLAIM + DETAILED DESCRIPTION]

To April Shaw
From C. Moroboshi
Total 8 pages

Translated: 05:39:39 JST 06/07/2007
Dictionary: Last updated 05/18/2007 / Priority: 1. Mathematics/Physics / 2. Electronic engineering / 3. JIS (Japan Industrial Standards) term

CLAIMS

[Claim(s)]
[Claim 1] The demand to an operating system from an application program, A demand taking-in means to take in the demand from an application program at at least one place among the demand to basic BIOS, and demand ** from an application program to hardware, The demand taken in by the above-mentioned demand taking-in means in a normal demand Or a request content distinction means to distinguish the demand by a computer virus, Computer virus invasion prevention equipment characterized by providing an output means by which this demand forbids the demand at least based on the distinction result of the above-mentioned request content distinction means in the demand by a computer virus.
[Claim 2] The demand to an operating system from an application program, The inside of the demand to basic BIOS from an application program, and the demand from an application program to hardware, the demand with a normal demand which took in the demand at at least one place, and was [above-mentioned / picking] crowded -- or [the demand by a computer virus / distinguish and] The computer virus invasion prevention method characterized by forbidding the demand at least in a demand according [the above-mentioned request content] to a computer virus.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to computer virus invasion prevention equipment and an invasion prevention method, and before a computer virus invades and increases especially, it relates to what checks this in advance and can prevent its invasion and multiplication.
[0002]
[Description of the Prior Art] Breakage of the program by a computer virus serves as a big social problem these days. A computer virus has self-proliferation potency power and infection capability here, here lets a network or a floppy disk pass, and says the malignant program which invades into other computers to it. As an infection route of this kind of computer virus, as described above, it is infected by invading through a network or using the floppy disk already polluted by the computer virus. When infected with a computer virus, condition that a message unnecessary on a screen will be displayed, a system error will increase unusually, the file memorized will be eliminated, or a hard disk will be damaged depending on the case will occur.
[0003] It was conventionally coped with by the following methods to invasion and multiplication of such a computer virus. First, write-protected operation of forbidding the writing from outside to various files is performed, and there is a method of preventing invasion to the file of a computer virus. Moreover, there is a method of checking the existence of infection of a file by reserving the normal file with which the computer virus is not infected, and comparing this normal file with the file

to be used. Furthermore, the history of a file operation is created and there is also the method of distinguishing whether it is infected with the computer virus by investigating the history.
[0004]
[Problem to be solved by the invention] According to the above-mentioned conventional composition, there were the following problems. All the conventional policies to invasion and multiplication of a computer virus were ex post. Namely, operate a file directly by arbitrary methods, check the existence of infection of a computer virus, and now Even if it could not prevent invasion and multiplication of the computer virus in advance but could check the fact of infection of a computer virus by the conventional method, then, it may have been said that it had already spread widely.
[0005] There is a place which this invention was made based on such a point, and is made into the purpose in offering the computer virus invasion prevention equipment which makes it possible to check invasion of a computer virus in advance and to prevent its invasion and multiplication, and an invasion prevention method.
[0006]
[Means for solving problem] [the computer virus invasion prevention equipment by the invention in this application] in order to attain the above-mentioned purpose The demand to an operating system from an application program, A demand taking-in means to take in the demand from an application program at at least one place among the demand to basic BIOS, and the demand to hardware from an application program, The demand taken in by the above-mentioned demand taking-in means in a normal demand Or a request content distinction means to distinguish the demand by a computer virus, Based on the distinction result of the above-mentioned request content distinction means, this demand is characterized by providing an output means to forbid the demand at least in the demand by a computer virus.
[0007] [moreover, the computer virus invasion prevention method by this invention] The demand to an operating system from an application program, The inside of the demand to basic BIOS from an application program, and the demand from an application program to hardware, the demand with a normal demand which took in the demand at at least one place, and was [above-mentioned / picking] crowded — or the demand by a computer virus is distinguished and the above-mentioned request content is characterized by forbidding the demand at least in the demand by a computer virus.
[0008]
[Function] In the case of this invention, in at least one in a demand to an operating system, basic BIOS, or hardware, the demand is taken in from application. next, the thing which has the taken-in normal demand — or what was polluted by the computer virus is distinguished. A demand is forbidden when being polluted by the computer virus, as a result of distinguishing.
[0009] With reference to drawing 1 or drawing 12 , one working example of this invention is explained hereafter. First, with reference to drawing 1 , the outline of the equipment by this example and a method is explained. Usually, in the software which moves various computers and it, there is hardware 1 first. although this hardware 1 is ** of ****** which constitutes computer systems and is omitted by a diagram, it means the main part of a computer, a display, a printer, an external memory, communication equipment, etc.
[0010] There is software to the above-mentioned hardware 1, by this software, instructions are sent to the above-mentioned hardware 1, and a request is operated. As above-mentioned SOFUTOEA, as shown in a figure, there are application (application program) 3, an operating system 5, and basic BIOS 7. The above-mentioned application 3 is a program for the original purpose which is called the application program and usually uses a computer. Moreover, an operating system 5 is one of the basic programs, and in order to use the hardware 1 and software of a computer effectively, it performs comprehensive management. Furthermore, above-mentioned basic BIOS 7 is the program group which stored the basic motion of the computer, and is for controlling hardware 1. And an

operating system 5, basic BIOS 7, and hardware 1 are called suitably, or the above-mentioned application 3 operates them, and makes a request operate.
[0011] The arbitrary demands 9 are outputted to the OPERETEINGU system 5 from the above-mentioned application 3. Similarly, while the arbitrary demands 11 are outputted from application 3 also to basic BIOS 7, the arbitrary demands 13 are outputted from application 3 also to hardware 1.
[0012] Between the above-mentioned application 3 and the OPERETEINGU system 5, virus supervisory system A intervenes alternatively. This virus supervisory system A takes in the contents of the demand 9 by the demand taking-in means 15. what has the taken-in normal demand 9 — or [what is depended on a computer virus / with the demand distinction means 17 / distinguish and] In being the demand by a computer virus temporarily as a result of distinction, it outputs warning, while forbidding the demand to an operating system 5 from application 3 by the output means 19. Moreover, when normal, execution will be moved to an operating system 5. In addition, as the above-mentioned warning, a message can be displayed on a screen or what sounds a buzzer can be considered.
[0013] Moreover, between application 3 and basic BIOS 7, virus supervisory system B intervenes alternatively. Furthermore, between application 3 and hardware 1, it is constituted so that virus supervisory system C may intervene alternatively. These virus supervisory system B and virus supervisory system C like the case of the above-mentioned virus supervisory system A Demand 11 or 13 is taken in by the demand taking-in means 15, and the taken-in demand 11 or 13 is distinguished by the demand distinction means 17, and in being the demand by a computer virus as a result of the distinction, while forbidding a demand by the output means 19, it outputs warning.
[0014] Next, above-mentioned virus supervisory system A, B, and C explain in what kind of procedure it is incorporated in the system with reference to drawing 2 , after switching on the power supply of a computer. First, a power supply is switched on and it is "started." Next, while virus supervisory system C suitable for hardware 1 is introduced, maintenance of basic BIOS 7 is performed. Next, distinction of whether maintenance of basic BIOS 7 was completed is made. Maintenance of basic BIOS 7, or when it completes, virus supervisory system B suitable for basic BIOS 7 is introduced. Moreover, when maintenance of basic BIOS 7 is not completed, basic BIOS 7 is fixed again.
[0015] Next, the OPE rating system 5 is fixed. When maintenance of an operating system 5 is completed, virus supervisory system A suitable for an operating system 5 is introduced. When maintenance of an operating system 5 is not completed, the OPERETEINGU system 5 is fixed again. And when introduction of virus supervisory system A is completed, inclusion of a system will be completed and it means that organization which supervises the demand from application 3 was made. Moreover, as already stated, each of virus supervisory system A, B, and C will choose and incorporate the thing of arbitrary kinds according to the kind of not one kind but the hardware 1, basic BIOS 7, and operating system 5. In addition, he is trying to record in this example on Rwhich does not illustrate these the processings of a series of0M He is trying to prevent rewriting by a computer virus by it.
[0016] Next, it explains what kind of method is taken concretely as virus supervisory system A, B, and C. First, it explains from the database method (the scanning method). This puts beforehand the computer program by various kinds of computer viruses in a database, memorizes it, and distinguishes whether it exists in the computer program which is a subject of examination. With reference to drawing 3 , it explains hereafter. First, a demand is taken in by the demand taking-in means 15. Next, the taken-in demand is analyzed and it is distinguished whether judgment is required. When judgment is not required, processing is continued as it is. On the other hand, when judgment is required, comparison with the data of the database memorized beforehand is performed. And when a demand and the data put in a database are not in agreement, processing is continued as it is. Moreover, when a demand and the data put in a database are in agreement, while a demand is forbidden, warning and an inquiry are performed. Next, it is distinguished whether it continues by

checking processing. A process will be interrupted when it is judged that it does not continue.
[0017] It seems that it is shown in drawing 4 when comparison and distinction with the data put [above-mentioned] in a database are shown in more detail. First, reading of a file is performed. Next, the first data is taken out out of a database. And it is distinguished whether the read contents of a file are compared with the taken-out data, and it is in agreement. When in agreement, it judges as "STC, i.e., the thing infected with the computer virus." On the other hand, when not in agreement, it is distinguished whether it compared with all the data in a database. the case where it compares with all the data -- "CLC" — that is, it is judged that it is normal. When not comparing with all data, comparison with the following data is performed. That is, the following data is taken out out of a database and comparison with the read file is performed. Thus, the existence of infection of a computer virus is distinguished by comparing with all the data of the database.
[0018] Next, distinction by the backing-up method is explained with reference to drawing 5 and drawing 6 . With the backing-up method, the backup file of the file used as a subject of examination is created and saved beforehand. That is, all or the information which processed the contents of a file in part on files is used as a backup file, and is created and saved beforehand. The rest compares a file and the above-mentioned backup file to be examined, and distinguishes whether it is normal.
[0019] Hereafter, if it explains in detail with reference to a figure, as shown in drawing 5 , creation of a backup file will be started first. That is, the total value of SUM calculation, i.e., the byte of a file, is calculated by reading the contents of a file. And SUM data is outputted and the SUM calculation and filename are recorded on the backup file (disk). Creation of backup file ** is completed by this.
[0020] next, the account of the upper — distinction by the backing-up method which uses the backup file currently created beforehand is explained with reference to drawing 6 . First, data is read from a file to be examined. Next, SUM calculation is performed based on the read data. Next, the calculated value and the calculated value taken in from the backup file are inputted, and distinction of whether to be in agreement is made. And when not in agreement, it is judged as "STC, i.e., the thing infected with the computer virus." moreover -- the case of being in agreement -- "CLC" — that is, it is judged that it is normal.
[0021] Next, the case where vaccine law is adopted with reference to drawing 7 or drawing 10 is explained. This vaccine law inoculates beforehand the program which distinguishes the existence of infection of a virus into the file which becomes a subject of examination, and makes the file itself distinguish the existence of infection of a virus at the time of a system startup. First, the usual file 21 is shown in drawing 7 , and only the original former program 23 is recorded. The SUM data 25 and the check program 27 are inoculated into this file 21, and the inoculated file 29 is created. Drawing 9 showed the creation process of this inoculation file 29. That is, reading of a former program file is performed, next SUM calculation is performed. Next, a check program is added while SUM data is added to the end of a file. And the head of a file is jumped to a check program and creation of the inoculation file 29 is completed.
[0022] Next, the inoculation file 29 explains at what kind of process the existence of infection of a computer virus is distinguished in person. If the inoculation file 29 is performed as shown in drawing 10 , a check program will start. And at the time, SUM of the former program 23 is calculated and the SUM value currently beforehand recorded as the calculated value is compared. And the former program 23 is started noting that it is normal, when in agreement. On the other hand, subsequent execution is stopped noting that the former program 23 is polluted by the virus, when not in agreement.
[0023] Next, the case where the keyword method is adopted is explained. This keyword method is a method of forbidding specific operation by a keyword, and when a keyword is in agreement using arbitrary keywords, it permits subsequent operation. With reference to drawing 11 , it explains hereafter. This shows the case where it carries out to the file write-in demand in service of MS-DOS (registered trademark), and a write-in demand (AH=40) is advanced first. Next, it is judged as what is infected with the virus when password inspection is conducted and a password is not in

agreement, and when in agreement, it is judged that it is normal.
[0024] Next, the case where adjective law is adopted is explained. That is, a difference is in a process by the case where it is polluted by the computer virus, and the case of being normal. By checking this, it is distinguished whether it is infected with the computer virus. When the open demand (AX=3D02) which can be file written in is specifically required into the service demand of MS-DOS (registered trademark), for example, In being normal, it does not require the attribute of a file, but when polluted by the computer virus, attribute change (AX=4301) of a file is required immediately before. Therefore, it can be distinguished by whether attribute change of the above-mentioned file is required whether it is polluted by the computer virus. An example of the above-mentioned adjective law is shown in drawing 12 .
[0025] In addition, in virus supervisory system A, B, and C, you may adopt another methods other than these arbitrarily about whether it carries out by adopting which method out of an all directions method which was described above.
[0026] According to this example, the following effects can be done so above. First, check this, when the demand polluted by the computer virus is advanced from application 3, and it is distinguished whether it is polluted by the computer virus. Since it constitutes so that warning may be outputted while stopping a demand, when polluted While being able to discover whether application 3 is polluted by the computer virus at an early stage, invasion and spread of subsequent computer viruses can be prevented in advance. Since it is made to check existence of infection by a computer virus within a system automatically especially, unlike checking ex post like before, the damage caused by invasion and spread of a computer virus can be kept to the minimum.
[0027] Moreover, since suitable virus supervisory system A, B, and C are chosen automatically and can be supplied by the operating system 5, basic BIOS 7, and hardware 1 to be used, usage is also good.
[0028] In addition, this invention is not limited to said one working example. For example, although it was made to make virus supervisory system A, B, and C intervene in said one working example between each of application 3, an operating system 5, basic BIOS 7, and hardware 1 as shown in drawing 1 The composition made to be placed between arbitrary parts out of them is also considered.
[0029]
[Effect of the Invention] As explained in full detail above, according to the computer virus invasion prevention equipment and the invasion prevention method by this invention, the existence of infection by a computer virus can be discovered at an early stage, and the invasion and spread after it can be prevented beforehand. Therefore, the damage caused by a computer virus can be made to reduce sharply compared with an ex post method like before.

[Translation done.]